PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGIRAN LA CONTRACTACIÓ DEL SERVEI DE SOC (SECURITY OPERATIONS CENTER) DE TECNOCAMPUS MATARÓ-MARESME

EXPEDIENT NÚMERO ES_LA0011122_2024_EXP_108

1 Objecte del contracte

La infraestructura tecnològica de TECNOCAMPUS suporta els sistemes d'informació que utilitzen els diferents serveis corporatius en la seva gestió diària. És per això, que aquesta infraestructura de sistemes i comunicacions esdevé un element clau que ha d'assegurar el suport tècnic especialitzat al més alt nivell possible amb l'objecte de garantir un servei continu i d'excel·lència. Sobre aquesta infraestructura s'implementen tots els serveis que TECNOCAMPUS actualment està oferint i per tant, requereixen el més alt nivell possible de protecció envers amenaces externes com son virus informàtics, ciberatacs o qualsevol mal us, sigui intencionat o no, dels recursos informàtics existents a TECNOCAMPUS per tal que el seu funcionament sigui adequat i de qualitat.

El Tecnocampus té en vigor actualment i fins a 15/07/2026 les llicències de programari de seguretat TrendMicro segons quadre de l'apartat 2.1. L'adjudicatari ha de constar com a "**GOLD Partner" de TrendMicro dins la plataforma Vision One** Els licitadors han de proposar una solució documentada de manera estructurada assumint la continuïtat del servei actual segons punt 2.1, gestió complerta del servei segons definit a punt 2.2, Pla de manteniment Correctiu, preventiu i proactiu segons punts 2.3, 2.4 i 2.5 respectivament, així com un pla de formació pels responsables del contracte segons punt 2.6. Aquesta proposta no podrà excedir del 20 pàgines i haurà de respectar la estructura indicada. Es requerirà també un pla de traspàs de servei segons indicat a punt 3.4, on no es podrà excedir les 4 planes.

El contracte tindrà per objecte la prestació del servei Centre d'operacions de seguretat pels serveis i usuaris de Tecnocampus Mataró-Maresme, en endavant SO per des de la data de signatura d'aquest contracte i fins al 15 de Juliol de l'any 2026, amb els termes contemplats en aquest plec de prescripcions tècniques.

El termini de durada del contracte serà de 24 mesos a partir del dia 15 de Juliol de l'any 2024

Els objectius d'aquest contracte serà la continuació dels serveis actualment prestats i millora del servei de seguretat tecnològica a tota la superfície TIC del Tecnocampus i sectors que tinguin una interacció directa amb els entorns TIC corporatius del tecnocampus que permetin portar el servei de SOC del Tecnocampus al màxim nivell d'excel·lència.

2 Descripció del servei

2.1 Estat actual

La estructura actual securitza l'entorn Tecnocampus des de una Base XDR que gestiona de manera proactiva els serveis de correu, Office 365, entorns cloud, servidors i tots els endpoints corporatius

Producte	Número de referencia únic (SKU)	quantitat
Apex One as a Service includes Mac, iDLP, iVP, iAC and Apex Central	OSHSWWMXXLIUSN	501
Trend Micro Cloud App Security	NNZBZZE1XLIUSN	751
Trend Micro Email Security - Standard	DFZBZZE1XLIUSN	751
Trend Micro Internet Security	TICIWWMFXLIULR	300
Cloud One - Workload Security (Deep Security as a Service) Pre-Paid Annual Subscription - per Servers, VMs or Cis	DXZYZZMAXLIESN	130
Managed XDR, Endpoints, Servers & Cloud Workloads (Messaging included): [Service]	MDEDRSEAYLIUSN	631
Trend Micro Vision One Credits	VOMMMMMXXLIPSN	14873

Figura 1 – Llicenciament en vigor durant tot el contracte

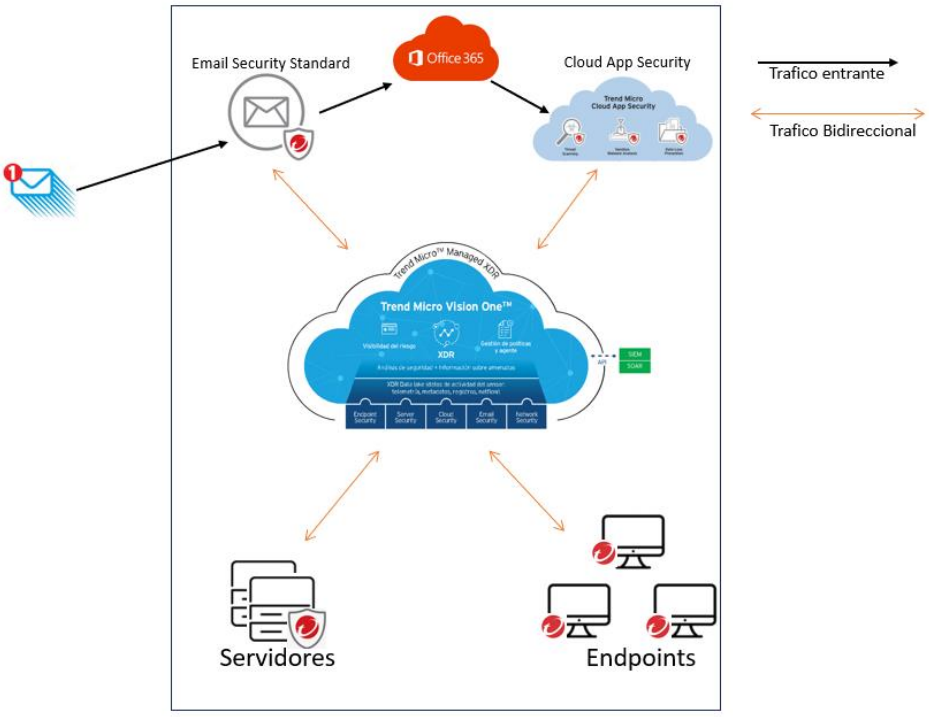

Figura 2 - Esquema serveis TrendMicro (Tecnocampus)

Email Security Standard: Solució de Gateway que aplica filtre d'IP, antispoofing, antispam, antiphishing i quarantena de seguiment de correus tant així com filtres de contingut.

Cloud App Security: Solució integrada a nivell d'API sobre office aplicant regles de seguretat sobre tràfic intern i aplicacions de Sharing com Teams, Sharepoint i OneDrive, utilitzant tecnologia d'Antispam, Antimalware i utilitzant una Sandbox integrada.

Cloud One Workload Security: Tecnologia desenvolupada per a servidors amb capacitat d'antimalware next gen aplicant analisi per mitjà d'IA, Firewall, Log Inspection, Monitor d'integritat i tecnologia de parxís virtual avançat protegint apps i el mateix OS.

Apex One: Tecnologia d' endpoint amb capacitats de Next Gen amb capacitats afegides de Device control, Aplication control, Firewall i IPS.

Vision One XDR: Plataforma Unificada amb tecnologia de correlació d'esdeveniments per a la detecció d'atacs que no utilitzen programari maliciós mitjançant l'ús de regla MITRE per a la mitigació proactiva d'amenaces o riscos de seguretat emergents permetent la creació de respostes automatitzades.

2.2 Servei Gestionat

El servei de SOC ha de ser completament gestionat, alliberant de totes les tasques operatives, manteniment preventiu, proactiu i correctiu al personal del Tecnocampus, que restarà amb un paper de gestor i control de l'entorn i del servei.

La proposta presentada ha de quedar estructurada seguint els punts indicats:

Serveis Proactius / Preventius

- Technical Account Manager
- Revisions d' infraestructura
- Implementació de totes les solucions TrendMicro
- Migracions de versions de productes TrendMicro
- Cicle anual de migracions de versions de productes

Serveis Correctius

- Suport davant emergència Remot 24x7
- Suport davant emergència OnSite 24x7

Serveis Resolutius

- Suport Resolutiu via Mail 9x5
- Suport Resolutiu telefònic 9x5
- Suport Resolutiu Remot 9x5
- Suport Resolutiu OnSite 9x5

Servei de Formació

- Capacitació d'administració – Nivell inicial

- Capacitacions personalitzades (de segon nivell)

Cal incloure dins del servei un Technical Account Manager (en endavant TAM) que lideri aquest servei gestionat per part de l'adjudicatari, esdevenint punt de contacte únic pel Tecnocampus i màxim responsable de la correcta execució i compliment dels compromisos definits a aquest contracte, tant a nivell d'implementació inicial completa, operació i explotació de totes les funcionalitats durant la vigència del contracte, assistència a reunions de seguiment periòdiques o específiques en temps i forma demanades pel Tecnocampus en cada cas, així com liderar i gestionar qualsevol intervenció preventiva, correctiva o pròpia de la explotació de la plataforma. **Aquest perfil ha de tenir una experiència mínima al servei indicat de no menys de 6 anys amb clients de dimensionament de llicències igual o superior a les indicades a punt 2.1.**

L'adjudicatari ha de presentar un pla de gestió del servei basat en els següents punts com a mínim, estructurats temporalment i amb fites ben marcades i informades

2.2.1 Etapa 1.

- El TAM assignat al compte coordinarà al costat dels administradors i responsables de les solucions Trend Micro un cronograma mitjançant el qual es portaran endavant les revisions d' infraestructura de tota la plataforma. Durant la revisió de cada consola, es realitzaran les següents tasques en relació directa amb les nostres tecnologies o l' entorn sobre el qual actuen:
    - Verificació d'últimes versions, hotfixes i pegats de les solucions.
    - Verificació de configuracions generals i específiques en cada entorn.
    - Anàlisi global de deteccions, esdeveniments i possibles riscos registrats en els productes.
    - Anàlisi d'oportunitats de millora per desviacions a les bones pràctiques proposades per Trend Micro.
    - Verificació de l'estat general de les actualitzacions en els productes.
    - Provisió d'informació específica per tal de planificar correctament plans d'acció i migracions necessàries

2.2.2 Etapa 2.

- Presentació d' estat i planificació anual conclosa l' etapa de revisions d' infraestructura, es presentaran les troballes i oportunitats de millores detectades en una reunió conjunta. Els objectius d'aquesta trobada seran:
- Compartir la totalitat de les troballes, per ordre de criticitat.
- Definir les accions immediates per a alertes de risc alt si existissin.
- Priorització de projectes, temps estimats i responsables.
- Planificació anual.

2.2.3 Etapa 3.

- Execució del pla anual d' acord amb la planificació anual proposada en l' etapa anterior, el TAM anirà coordinant les accions necessàries per avançar en els diferents projectes d' acord amb la priorització establerta
- Migracions de versions de producte.
- Correcció de configuracions
- Reenginyeries o canvis de topologia.
- POCs de noves tecnologies.

2.2.4 Etapa 4.

- Presentació d' estat final i recomanacions Finalitzats els projectes, es realitzarà una presentació final dels seus resultats. S' hi exposarà l' activitat de tot l' any i l' estat complet de la plataforma:
- Estat inicial de les solucions, a inicis del rellevament.
- Estat final de l'entorn després de l'execució dels projectes.
- Resultats de les POCs realitzades.
- Propostes de millora per a l'any vinent.

2.3 Manteniment Correctiu

En el moment de que de manera proactiva per part dels serveis del SOC o bé per una notificació del Tecnocampus es consideri que un comportament compatible amb una infecció o incident de seguretat dins de l'àmbit d'actuació de la plataforma gestionada per aquest contracte caldrà iniciar els procediments de avaluació, resolució i informe de les actuacions efectuades, afectacions mitigades i procediments de millora a executar dins del servei de SOC per evitar la seva reproducció.

El servei ha d'incloure específicament la assistència en casos urgents (24x7) no urgents (9x5) segons indicat a continuació:

2.3.1 Serveis davant d'incidents 24x7 (urgents)

- Situacions incloses:

    - **Infecció de virus**: Quan es detecti una amenaça dins de la xarxa del client i aquesta es trobi afectant servidors crítics de la companyia o un parc d' estacions de treball major al 10% o amb un mínim de cent equips infectats, comptabilitzant en tots els casos només equips protegits per la nostra solució.
    - **Comportament víric o anòmal a la xarxa**: Quan es presentin símptomes anòmals dins de la xarxa, els quals puguin ser directament relacionats amb noves amenaces i aquests símptomes afectin la continuïtat del negoci, denegant el servei d' enllaços, estacions de treball i serveis crítics per a la companyia.
    - **Inconvenients de producte** que ocasionin riscos a la continuïtat operativa de l' organització: En totes aquelles situacions on es provoqui talls en els serveis crítics protegits per les nostres solucions i on per alguna causa pugui provocar-se denegació de servei o caiguda dràstica del rendiment de la solució. Reportat l'incident, el tècnic de guàrdia realitzarà una anàlisi de la situació de manera remota (logs, configuracions i/o mostres de virus recol·lectades). En cas de no

poder brindar una solució adequada, es procedirà al tractament on site de l' incident. En tot moment es prioritzarà el temps de resolució de l' incident.

Davant qualsevol d'aquestes situacions s'haurà de donar un servei de suport 24x7 amb una anàlisi remota o on site si es determinés la necessitat per analitzar i solventar l'incident de seguretat aplicant la solució de workarround que es determini. No hi ha d'haver cap límit en les intervencions d'aquesta tipologia a aquest contracte, incloent actuacions dins o fora d'hores d'oficina, remotes o on-site a petició directa del responsable del contracte.

2.3.2 **Serveis Resolutius (no urgents)**

En assistències que no siguin considerats urgents caldrà oferir un servei en horari d'oficina per la atenció a possibles incidències menors, resolució de dubtes i qualsevol interacció del SOC sobre la que el responsable del contracte per part del Tecnocampus requereixi. Tots aquests serveis restaran inclosos al contracte sense representar cap sobrecost dins l'àmbit del servei contractat i de les eines que formin part de la plataforma SOC (llistades a punts 2.1 i 2.2 d'aquest document.

Suport Resolutiu 9x5 (de 9 a 18h) : Anàlisi i abordatge d' incidents de tot tipus que posin en risc la continuïtat de l' operació digital en serveis a l' empresa, que provoquin baix rendiment o que no permetin un ús adequat dels productes,

Modalitats de prestació:

- Atenció immediata telefònica i via mail pel nostre equip de suport tècnic.
- Sessions remotes compartides amb el client.
- Visites in situ.

En tot moment es prioritzarà la millor opció per arribar a la resolució de l' incident. Les visites en lloc s' hauran de coordinar amb una antelació de dos dies hàbils si és possible.

El Tecnocampus podrà fer ús del servei en qualsevol de les següents situacions:

- Anàlisi i/o resolució de casos oberts.
- Recol·lecció d'informació necessària per a l'obertura/anàlisi de cas.
- Aplicació de configuracions demanades per qualsevol de les parts.
- Neteja d' equips infectats

2.4 Manteniment Preventiu

L'adjudicatari haurà de presentar un pla de manteniment preventiu que asseguri un correcte funcionament i operació de tota la plataforma del SOC. Aquest pla s'implementarà el primer dia de contracte amb els serveis existents i incorporarà els nous serveis que es puguin incorporar durant la durada del servei.

Aquest pla de manteniment preventiu ha d'assegurar que tot el potencial de la plataforma està actiu conforme les necessitats de l'entorn del Tecnocampus, assegurant tot l'entorn tecnològic i serveis relacionats.

Aquest pla ha d'incorporar:

- Auditoria dels serveis actuals (punt 2.1), elaborant un informe específic on s'analitzi la seva definició i funcionament, detectant punts de millora i proposant els plans necessaris per assolir el màxim nivell d'eficiència. (4 setmanes des de inici de contracte)
- Llistat de tasques pròpies de manteniment de la plataforma per optimitzar el seu servei de securització, incloent els següents àmbits:
    - Plataforma Trend Micro i serveis
    - Servidors de la plataforma
- Informes de seguiment de projecte (punt 2.9)

Dins d'aquets manteniment també quedaran incorporades totes les configuracions i canvis dels serveis de la plataforma que siguin necessaris per disposar en tot moment de la millor solució de SOC possible. La implementació i manteniment dels canvis o millores que siguin considerades dins aquest pla queden incloses dins del contracte sempre que els serveis i llicències vigents ho permetin.

2.5 Manteniment Proactiu

El nivell de proactivitat assumit per la proposta presentada serà considerat com a crític i determinant tant en la valoració de les propostes dels licitadors com a la avaluació continuada del mateix. La proposta de manteniment proactiu ha de considerar els nivell de monitorització dels serveis del SOC, de les incidències de seguretat i comportaments anòmals, així com el nivell de millora contínua del SOC, fent partícip al responsable del contracte en tot moment de l'estat actual i propostes de millora i optimització dels serveis de la plataforma, en reunions mensuals o a demanda per qualsevol de les dues parts. De la mateixa manera qualsevol millora o novetat de Trend Micro aplicable haurà de ser traslladada i valorada si el TCM ho considera oportú. Qualsevol servei afegit quedarà inclòs als serveis preventius, correctiu i proactius del servei de manera immediata.

2.6 Formació personal TCM (SIT)

L'adjudicatari haurà de proporcionar el nivell de formació i transferència de coneixement adient al personal responsable del contracte per poder assumir les tasques pròpies de la gestió del servei, així com una operació suficient de la plataforma del SOC, basada en els següents punts:

- Interpretació d'arxius d'esdeveniments
- Administració de la consola
- Formacions específiques a demanda de Tecnocampus

2.7 Reunions de seguiment

Es faran reunions del seguiment del servei amb el personal de Tecnocampus de forma mensual, encara que aquesta periodicitat podrà ser modificada a criteri de Tecnocampus. En aquestes reunions intervindrà el responsable del servei i el personal que Tecnocampus designi. L'objectiu de les reunions periòdiques és revisar el grau de compliment dels objectius, les especificacions funcionals i la validació de la programació de les activitats realitzades. L'adjudicatari generarà una acta de reunió el les 48 hores posteriors on quedin reflectits tots els punts tractats a la reunió, conclusions i tasques pendents.

2.7.1 Reunions de seguiment SOC – Servei de Xarxa

El servei gestionat del SOC tindrà evidents sinèrgies amb el servei de seguretat Perimetral (Firewall) i de LAN del Tecnocampus. Es requerirà una col·laboració habitual entre els dos serveis a fi d'aconseguir una solució de seguretat òptima aprofitant les fortaleses de les dues solucions i evitant processos o polítiques de seguretat repetitives o innecessàries. TecnoCampus establirà una periodicitat de reunions remotes (o presencials si al criticitat ho requereix) entre els responsables o equip tècnic si es determina dels dos serveis que quedaran incloses dins dels serveis contractats i on es tractaran els punts que TecnoCampus consideri necessaris o els que proposin qualsevol dels assistents.

2.8 Informes de seguiment:

L'adjudicatari es compromet a generar informes que inclouran com a mínim les següents dades:

- Estat i evolució dels diferents serveis del SOC
- Incidències de seguretat i procediments aplicats.
- Tasques programades (executades i planificades)
- Interaccions amb altres serveis
- Propostes de millora
- Altres

Aquests informes hauran de ser entregats i posats a la disposició de TECNOCAMPUS, per ser revisats i analitzats quan sigui necessari.

3 Paràmetres de gestió de la qualitat del servei

Els següents aspectes i indicadors seran un referent per avaluar la correcta gestió de la qualitat del servei i seran revisats de forma mensual pel Tecnocampus. Es consideraran els indicadors d'incidències, seguiment del servei i interaccions amb el servei gestionat de seguretat Perimetral i LAN/WAN del TCM i el seu temps de resposta i resolució.

3.1.1 Incidències

Es classificaran els diferents tipus d'incidències segons la seva criticitat:

- **Urgent:** Les tipificades segons punt 2.3.1
- **Normal:** Les tipificades segons punt 2.3.2

3.1.2 Seguiment del servei

Es classificarà el nivell de servei gestionat conforme el temps de resposta i resolució de les consultes efectuades pel personal del TCM. Totes les consultes es consideraran sota la mateixa criticitat normal.

3.1.3 Interaccions amb servei de seguretat Perimetral i LAN/WAN

Els servei gestionat del SOC i el de Seguretat Perimetral requeriran d'una interlocució i seguiment comú evident i serà responsabilitat dels dos gestors establir les vies de comunicació adient per assolir aquesta sinèrgia del tot necessària, en tot moment gestionada pel responsable de contracte del Tecnocampus. En qualsevol moment i sota petició de qualsevol de les parts es pot iniciar una comunicació per solucionar una incidència, gestionar una petició d'informació o qualsevol consideració necessària pel bon funcionament dels dos serveis. Es considera crítica aquesta col·laboració i per això es defineixen els indicadors de seguiment següents:

- Urgents: Requeriments per solucionar incidències de servei que tinguin afectació greu (serveis indisponibles)
- Normals: Requeriments d'informació, configuracions, tasques programades o reunions de seguiment

3.2 Temps de resposta i temps de resolució

Es defineix com a **Temps de Resposta** el període entre la recepció per part de l'adjudicatari als seus sistemes de monitorització (incidències) o bé per les vies de comunicació habituals (trucada telefònica i/o email) per peticions de seguiment de servei o interaccions amb el Servei de seguretat Perimetral.

Es defineix com a Temps de Resolució el període entre la seva recepció i la recuperació del servei afectat una vegada aplicats els procediments adients en el cas de les incidències i del període entre la recepció de la notificació i la seva resposta fonamentada i/o resolutòria.

SLA incidències		
Tipus	**Temps resposta**	**Temps resolució**
Urgent	< 5'	< 30'
Alta	< 15'	< 240'

Figura 3 - SLA Incidències

SLA Seguiment Servei		
Tipus	**Temps resposta**	**Temps resolució**
Estàndard	< 30'	NBD

Figura 4 - SLA Seguiment Servei SOC

SLA Interaccions SSP		
Tipus	**Temps resposta**	**Temps resolució**
Urgent	< 5’	< 30’
Alta	< 15’	< 240’

Figura 5 - SLA Interaccions SSP

Els acords de servei aquí indicats hauran de ser d’obligat compliment per l’adjudicatari i seran auditats i penalitzats en cas d’incompliment segons referit a la documentació d’aquest contracte

3.3 Seguretat i confidencialitat de la informació

L'adjudicatari està expressament obligat a mantenir una confidencialitat absoluta i reserva sobre qualsevol dada que pugui conèixer amb motiu de l'execució del contracte. L'adjudicatari estarà obligat a complir amb el que estableix la Llei Orgànica 3/2018, de 5 de desembre, sobre protecció de dades personals i garantia de drets digitals.

3.4 Finalització i transferència del servei

En cas de finalització del contracte l’adjudicatari restarà obligat a efectuar un traspàs de coneixement al nou prestatari de manera adequada per assegurar que el SOC no es veu afectat ni pel canvi de prestatari ni per el possible canvi de plataforma. Aquest període de traspàs de coneixement serà de 4 setmanes (iniciant 2 setmanes abans de la finalització del contracte actiu), o es proporcionarà al nou adjudicatari tota la informació que requereixi per assegurar la continuïtat del servei sota control del personal responsable del TCM. Aquesta informació inclourà, com a mínim els informes de seguiment mensuals i anual del del servei, operatives habituals, recursos assignats, incidents de seguretat reportats i tractament aplicat en informe específic, així com tota la informació que es consideri necessària validada pel responsable del contracte.